Аннотация дисциплины

Наименование дисциплины	**Криптографические методы защиты информации**
Содержание	Основные понятия криптографии. Классические шифры замены. Классические шифры перестановки. Принципы построения современных шифров с симметричным ключом. Современные стандарты симметричного шифрования DES, AES, ГОСТ 28147-89, ГОСТ Р 34.12-2015. Современные алгоритмы шифрования с открытым ключами. Криптосистемы RSA, Эль-Гамаля, Рабина. Алгоритмы генерации простых чисел. Проверка чисел на простоту. Сложность криптографических алгоритмов. Аутентификация данных. Электронная цифровая подпись. Алгоритмы ЭЦП: RSA, Эль-Гамаля, Шнорра, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012. Атаки и угрозы схемами ЭЦП. Понятие о структуре и способах построения криптографических протоколов. Классификация криптографических протоколов.
Реализуемые компетенции	способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2) способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4) способностью применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем (ПСК-2)
Результаты освоения дисциплины (модуля)	**ОПК-2** **Знать:** сведения из математических дисциплин, позволяющие решать профессиональные задачи, **Уметь:** применять соответствующий математический аппарат для решения профессиональных задач, **Владеть:** методами из математических дисциплин для решения профессиональных задач. **ПК-4** **Знать:** основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; - правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; - принципы и методы организационной защиты информации; **Уметь:** формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; - анализировать и оценивать угрозы информационной безопасности объекта;

	Владеть: навыками работы с нормативными правовыми актами; - навыками организации и обеспечения режима секретности; - методами формирования требований по защите информации; - методами организации и управления деятельностью служб защиты информации на предприятии; - методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; **ПСК-2** **Знать:** современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем, **Уметь:** применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем, **Владеть:** способностью применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем
Трудоемкость, з.е.	6 з.е.
Форма отчетности	Экзамен – 6 семестр, Зачет с оценкой – 5 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Петров А.А. Компьютерная безопасность. Криптографические методы защиты.- Саратов: Профобразование, 2017.- 446 с.
Дополнительная литература	1. Лапонина О.Р. Криптографические основы безопасности.- Москва: ИНТУИТ, 2016.- 244 с. 2. Калмыков И.А. Криптографические методы защиты информации.- Ставрополь: СКФУ, 2015.- 109 с.